Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Data Exchange Policy

1.0. Statement

1.1. The Office of Information Technology (OIT) adopts all necessary measures to ensure that data exchanges with Maine State information assets comply with all relevant Federal and State Laws, as well as the industry best practices of Privacy and Security.

2.0. Background

2.1. The citizens of Maine trust their government with an immense cache of their data. It is essential for the State to reciprocate that trust with the best possible stewardship of that data.

2.2. Quality information is critical to effective government decision-making and fulfilling the government's obligation to its citizenry. This often necessitates exchanging data amongst the various agency information assets, as well as with external sources of information. It is essential that such exchanges comply with all relevant Federal and State Laws, Regulations, Statutes, and Rules, as well as the industry best practices of Privacy and Security.

2.3. Agencies are the caretakers of the data that they transact. While OIT handles the technical details, the Agency business units remain the fiduciary steward and custodian of their data.

3.0. Definitions

3.1. *Ad-hoc Data Exchange:* Any data exchange that is episodic and/or occasional. It is not economical to setup an automated process for such a transaction.

3.2. *Authorized Custodian:* An agency personnel who is empowered by a Federal or State Law, or Regulation, or Statute, or Rule, to asset stewardship of particular data transacted by that Agency.

3.3. *Data Classification:* The taxonomy of organizing data into categories, so that data may be used and protected efficiently. OIT has adopted the Federal Homeland

Security Traffic Light Protocol[1] for this purpose. Thus, there are four classifications of data, elaborated below:

3.3.1. *Internal Data (TLP: Green):* Data suitable for State employees, but not sensitive. Examples include employee newsletters and announcements, internal memoranda not classified as Sensitive or Confidential, etc.

3.3.2. *Public Data (TLP: White):* Data which is suitable for unrestricted public consumption. Examples include anything hosted on Maine.Gov which does not require an additional login.

3.3.3. *Sensitive Data (TLP: Amber):* Data suitable for State employees only. Leakage could cause unnecessary turmoil or confusion to the State, but no regulatory penalty. Examples include anything hosted on the State of Maine Intranet which does not require an additional login.

3.3.4. *Restricted Data (TLP: Red):* Data deserving the maximum Confidentiality, as determined by Federal and State Laws, Regulations, Statutes, and Rules. Access to such data must be granted only on an as-needed basis, and must be restricted as narrowly as possible to perform essential government functions. See further at Personally Identifiable Information (PII).

3.4. *Net-New Data Exchange:* Any data exchange that did not exist heretofore, and is commencing for the first time.

3.5. *Personally Identifiable Information (PII):* Information that can be used on its own, or in combination with other information, to identify, contact, or locate a single person, or to identify an individual in context. Refer to Paragraph 6 of Maine Public Law 10 MRSA § 1347[2] for a more detailed definition. PII includes, but is not limited to, Protected Health Information (PHI), Federal Tax Information (FTI), and Federal Education Rights and Privacy Act (FERPA) Information.

3.6. *Standing Data Exchange:* Any data exchange that is meant to transpire at a fixed frequency, over a long period of time. This is likely accomplished through an automated process.

4.0. Applicability

4.1. This policy applies to:

4.1.1. Any data exchange that either originates or terminates with the Maine State Executive Branch, involving data classified as either Sensitive (TLP: Amber) or Restricted (TLP: Red);

4.1.2. All State of Maine Executive Branch personnel, both employees and contractors; and

[1] https://www.us-cert.gov/tlp

[2] http://www.mainelegislature.org/legis/statutes/10/title10sec1347.html

4.1.3. Executive Branch Information Assets, irrespective of hosting location.

5.0. Responsibilities

5.1. *Agency Management:*

5.1.1. Ensure that they have the authority to transact the data exchange, in accordance with all relevant Federal and State Laws, Regulations, Statutes, and Rules.

5.1.2. Ensure that every net-new, standing data exchange is undertaken according to a signed Memorandum of Agreement (MoA).

5.2. *Chief Information Officer:*

5.2.1. Owns, executes, and enforces this Policy.

5.3. *OIT Management:*

5.3.1. Ensures that the underlying technical details of the actual exchange complies with the industry best practices of Security and Privacy.

6.0. Directives

6.1. No net-new, standing data exchange can commence without a signed Memorandum of Agreement (MoA) amongst the Authorized Custodians of the transacted data. Exempted are cases where both the sender and receiver happen to be the same authorized custodian.

6.2. For a new-new, standing data exchange, the disposition of the data by the receiver is strictly in accordance with the signed Memorandum of Agreement (MoA).

6.3. Exchange of data can happen only after Authentication, and must be explicitly documented. The documentation burden is two-fold. First, the data exchange must be documented in the enterprise application repository. Second, each instance of the data exchange must be documented in a transactional log (most likely, the enterprise file transfer log). The purpose of documenting in the enterprise application repository is to identify this data exchange as an active enterprise data sharing, whereas the purpose of documenting in the transactional log is to meet the audit burden that this instance of data exchange did actually transpire.

6.4. All data exchanges transpire via industry-standard protocols, such as Web Services, HTTPS, FTPS, and SFTP. Per NIST 800-52[3], the minimum acceptable level of dynamic encryption is TLS 1.2.

6.5. Any ad-hoc external exchange happens through the State of Maine Office 365. Ad-hoc, one-to-one external exchange happens through the user's OneDrive. Ad-hoc, one-to-many external exchanges happen through departmentally-approved SharePoint Sites and Document Libraries.

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

6.6. For any exchanged data, by default, the payload must be encrypted in-flight to the AES-256 standard, and the encryption key must be communicated separately from the payload. This directive may be superseded by a more specific instruction contained in relevant Federal and State Laws, Regulations, Statutes, and Rules.

7.0. Document Information

7.1. Initial Issue Date: 20 March 2020
7.2. Latest Revision Date: 20 March 2020
7.3. Point of Contact: Enterprise.Architect@Maine.Gov
7.4. Approved By: Chief Information Officer, OIT
7.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[4]
7.6. Waiver Process: Waiver Policy[5]

[4] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[5] https://www.maine.gov/oit/policies/waiver.pdf

8.0. Sample Data Exchange Memorandum of Agreement

MEMORANDUM OF AGREEMENT (MOA)
BETWEEN
MAINE DEPARTMENT #1, AND
MAINE DEPARTMENT #2,
FOR THE EXCHANGE OF ARMADILLO DATA

8.1. Parties

8.1.1. The Maine Department #1 is authorized to collect and maintain Armadillo data, consistent with applicable State and Federal Laws.

8.1.2. The Maine Department #2 develops and disseminates conservation information to local officials, employers, educators, and the public, in making decisions that promote economic opportunity and efficient use of natural resources.

8.2. Purpose

The purpose of this MoA is to document the rules under which the Parties enumerated above shall transact Armadillo Data. Maine Department #1 must meet reporting and accountability measures required by the Armadillo Innovation and Opportunity Act 2019. The reporting requirements of this Law (Title I, Chapter 4, Section 116) cannot be met without data sharing with Maine Department #2. Hence, the Maine Department #1 will transmit enumerated elements of Armadillo PII to Maine Department #2.

8.3. Legal Authority

Consistent with the Family Educational Rights and Privacy Act (FERPA)[6], the Maine Department #1 may disclose Armadillo PII to its authorized partners in connection with enumerated Federal and State programs. See 20 U.S.C. §1232g(b)(3)[7] and 34 CFR Part 99.31(a)(3)[8].

8.4. Agreement Administrators

Each Party has assigned one Agreement Administrator to act on its behalf. It is the Agreement Administrators' responsibility to ensure compliance with this MoA, and to serve as the official points-of-contact.

Agreement Administrator for Maine Department #1:
Name: _____
Title: _____
Address: _____

[6] https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[7] https://uscode.house.gov/view.xhtml?req=(title:20%20section:1232g%20edition:prelim)
[8] https://www.law.cornell.edu/cfr/text/34/99.31

Telephone: _____
Email: _____

Agreement Administrator for Maine Department #2:
Name: _____
Title: _____
Address: _____
Telephone: _____
Email: _____

8.5. Records Transacted

8.5.1. Armadillo First Name
8.5.2. Armadillo Middle Initial
8.5.3. Armadillo Last Name
8.5.4. Armadillo ID Number
8.5.5. Armadillo Date of Birth
8.5.6. Armadillo Finishing School (if available)

8.6. Terms and Conditions

The receiving party, i.e., Maine Department #2, understands, and agrees to:

8.6.1. Comply with the provisions of FERPA, and applicable State Laws, in all respects. For the purposes of the MoA, FERPA includes all requirements of 20 U.S.C. § 1232g, and 34 CFR Part 99, and any amendments thereto. Nothing in this MoA may be construed to maintain, use, disclose, or share data, transacted under this MoA, in a manner *not* allowed by FERPA.

8.6.2. Require all employees, contractors, and agents of Maine Department #2 to comply with this MoA, and all applicable provisions of FERPA, and other Federal and State Laws, with respect to the data transacted under this MoA. Maine Department #2 agrees to require of, and maintain, an appropriate confidentiality agreement with each employee, contractor, and agent with access to data transacted under this MoA. Nothing in this section authorizes Maine Department #2 to share data transacted under this MoA with any other individual, or entity, for any purpose, other than the enumerated Purpose of this MoA.

8.6.3. Nothing in this MoA can be construed to authorize Maine Department #2 to have access to additional data from the Maine Department #1.

8.6.4. Nothing in this MoA can be construed to convey ownership of the transacted data to Maine Department #2.

8.6.5. Maintain all data transacted under this MoA separate from all other data possessed by the Maine Department #2, and not copy, reproduce, or transmit

data transacted under this MoA, except as necessary to fulfill the enumerated Purpose of this MoA.

8.6.6. Not disclose the data transacted as part of this MoA in any manner that could identify any individual Armadillo, except as authorized by FERPA, to any entity other than authorized employees, contractors, and agents of Maine Department #2, for the enumerated Purpose of this MoA. The determination of whether a disclosure is authorized by FERPA shall be made by the Maine Department #1. Persons participating in approved work on behalf of the Parties under this MoA shall neither disclose, or otherwise release, data relating to an individual Armadillo, nor disclose information relating to a group of Armadillos, without ensuring the confidentiality of Armadillos in that group. Publications and reports of this data and, information related to it, including preliminary project descriptions, and draft reports, shall involve only aggregate data, and no PII, or other information that could lead to the identification of an Armadillo. No report of these data, even in the aggregated form, shall be released to anyone, unless Maine Department #2 receives prior written approval from the Maine Department #1.

8.6.7. Provide the Maine Department #1 with electronic copies of the final versions of all reports prior to their presentation or release in order to allow the Maine Department #1 to review the compliance with this MoA. Maine Department #1 reserves the right to distribute, and otherwise use, any report, or other associated documents, as it wishes, in sum, or in part.

8.6.8. Permit the Maine Department #1 to review Maine Department #2's policies and procedures regarding PII, and seek written assurances from Maine Department #2 that data transacted under this MoA is properly handled. Maine Department #2 is expected to maintain strict policies and procedures to ensure that all data transacted under this MoA is maintained in a secure manner that prevents further disclosure of the data, including the interception, diversion, duplication, or other unauthorized access.

At a minimum, Maine Department #2 agrees to comply with the following:

8.6.8.1. Data storage administration will include the strict control of all storage media. All storage media must be inventoried on an annual basis, or sooner, as dictated by clients, regulatory or other contractual agreements.

8.6.8.2. To the maximum extent possible, physical backup and transfer must be avoided, in favor of electronic transfer of encrypted backup files.

8.6.8.3. All data files and databases containing PII data will be encrypted at rest,

using at least AES-256 encryption, or better, before being electronically transferred across any network, internal or public.

8.6.8.4. All data files and databases that contain PII data that are backed up to physical media for transfer to offsite storage, must be backed up using at least AES-256 encryption, or better. No unencrypted intermediate backup files may be created.

8.6.8.5. Physical media containing PII data must be maintained in a secure environment prior to its transfer offsite.

8.6.8.6. Physical media containing PII data must be monitored during the internal shipping process, and must never be left unattended before handoff to the shipper.

8.6.8.7. Physical media containing PII data must be shipped in locked containers with no special markings, or other indications of the sensitive nature of the contents.

8.6.8.8. Shipping procedures must include a positive acknowledgement of receipt of encrypted media at the destination.

8.6.9. With respect to a suspected breach of data transacted under this MoA, report in detail to the Maine Department #1's Agreement Administrator within twenty-four (24) hours of first knowledge. It is also the responsibility of Maine Department #2 to develop a collaborative and expeditious remediation plan for the incident.

8.6.10. When the data transacted under this MoA is no longer needed for the enumerated Purpose of this MoA, destroy it completely, including any archival/backup copies, per the DOD 5220.22-M Media Sanitization Protocol[9]. Nothing in this MoA authorizes Maine Department #2 to maintain data transacted under this Moa beyond the time-period reasonably needed to fulfill the enumerated Purpose of this MoA, and, in no case, beyond the termination date of this MoA. Any destruction of this data must be witnessed by one other person who can later attest that a complete destruction of the data did transpire. Maine Department #2 agrees to submit a letter to the Maine Department #1, within 30 days of the termination of this MoA, attesting to this data destruction.

8.6.11. This MoA takes effect immediately upon signature by the authorized representative of each Party, and shall remain in effect until completion of the

[9] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf

enumerated Purpose of this MoA, or until canceled by either Party upon 30 days' written notice. This MoA may be amended, or renewed, at the discretion of the Parties.

8.6.12. This MoA contains the entire agreement of the Parties, and shall not be modified or altered, except in writing, executed by the authorized representative of the two Parties, and in a manner consistent with applicable State and Federal Laws, Regulations, Statutes, and Rules.

8.6.13. No delay or omission by either Party in exercising any right under this MoA can be construed as a waiver of that, or any other right. A waiver or consent given by either Party, on any one occasion, is effective only in that instance, and will not be construed as a bar to, or a waiver, of any right, on any other occasion. Neither the review, or approval, or acceptance, or payment, of any services under a separate Agreement, will be construed to operate as a waiver of any rights, or of any course of action, available under this MoA.

8.6.14. Any ambiguity in this MoA will *not* be construed against the Maine Department #1, but will be resolved by applying the most reasonable interpretation under the circumstances.

8.6.15. If any part of this MoA is held void, illegal, unenforceable, or in conflict with any Law, the validity of the remainder of this MoA will not be affected.

In witness whereof, the Parties have executed this MoA on the dates noted below:

Signatory for Maine Department #1:
Signature: _____
Name: _____
Title: _____
Date: _____

Signatory for Maine Department #2:
Signature: _____
Name: _____
Title: _____
Date: _____